Safety and availability of machinery.

Safety Integrity Level SIL
Performance Level PL
The EC Machinery Directive stipulates machinery should not present a risk – risk assessment to EN 1050 and EN ISO 14121-1. Since there is no zero risk, the aim is to achieve an acceptable residual risk. If safety is dependent on control systems, these must be designed so as to minimise malfunction.

Safety-related parts of machine control systems used to be designed to EN 954-1. This was based on the calculated risk (formed in categories). The aim was to set an appropriate behaviour (“control category”) against a category.

New electronics, above all the programmable controllers, could not be measured in terms of the simple category system found in EN 954-1. Test interval, lifetime and probability of failure were, for example, not considered in the old standard.

Help is now available from EN 62061 and EN ISO 13849-1, the successor standard of EN 954-1. The classification is made either in the Safety Integrity Level (SIL 1-3 in EN 62061) or in the Performance Level (PL a-e in EN ISO 13849-1).

### Step by step to safety – Step 1

**Risk assessment to EN 1050 / EN ISO 14121-1**

Without any protective measures a risk will lead to harm. Therefore the designer has to assess the risk as below:

- establish the limits and the intended use of the machinery
- identify any hazardous situations
- assess the risk for each hazard identified
- estimate the risk and decide on the need for risk reduction
4. Does application software have to be certified? If yes, to what standard?

A relationship between PL and SIL can be established through the PFH value.

```
<table>
<thead>
<tr>
<th>PL</th>
<th>Average probability of a dangerous failure per hour</th>
<th>SIL to EN 62061</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>10^{-5} ≤ PFH &lt; 10^{-4}</td>
<td>–</td>
</tr>
<tr>
<td>b</td>
<td>3 · 10^{-6} ≤ PFH &lt; 10^{-5}</td>
<td>SIL1</td>
</tr>
<tr>
<td>c</td>
<td>10^{-6} ≤ PFH &lt; 3 · 10^{-5}</td>
<td>SIL1</td>
</tr>
<tr>
<td>d</td>
<td>10^{-7} ≤ PFH &lt; 10^{-6}</td>
<td>SIL2</td>
</tr>
<tr>
<td>e</td>
<td>10^{-8} ≤ PFH &lt; 10^{-7}</td>
<td>SIL3</td>
</tr>
</tbody>
</table>
```

PFH: Probability of failure per hour (average probability of a dangerous failure per hour)

5. What does the letter “d” mean on MTTFd?

“d” stands for “dangerous”, the MTTFd describes the mean (statistical) time to a dangerous failure.

6. What difference is there between reliability and safety?

Reliability: Total of characteristics referring to the suitability for fulfilling the requirements at given conditions for a given time interval.

Safety: Circumstances under which the risk is not greater than the limit risk, include the ability not to cause or not to let occur any risk for a given period of time within defined limits.

7. Are safety modules required for the operation of machinery / plant?

No. Standard components may be used for the operation of machinery / plant.
This standard may be applied to safety-related parts of control systems and all types of machinery regardless of the type of technology and energy used (electrical, pneumatic, hydraulic, mechanical, etc).

This standard is to be applied to safety-related electrical, electronic and programmable control systems for machines.

Step 2
Defining the measures required to reduce the calculated risks

The objective is to reduce risk as much as possible, taking various factors into account.
- safety of the machine in all phases of its mission time
- ability of the machine to perform its function
- user friendliness of the machine

Only then shall the machines manufacturing, operating and disassembly costs be taken into consideration.

The hazard analysis and the risk reduction process require hazards to be eliminated or reduced through a hierarchy of measures:
- hazard elimination or risk reduction through design
- risk reduction through protection devices and additional protective measures
- risk reduction through the availability of user information about residual risk

Step 3
Risk reduction through control measures

If the risk is to be reduced by taking control measures, the design of safety-relevant control units is an integral part of the whole design procedure for the machine.

The safety-relevant control system will provide the safety function(s) with a SIL or PL which achieves the necessary risk reduction.

Step 4
Implementation of control measures using

EN 62061:

This standard is to be applied to safety-related electrical, electronic and programmable control systems for machines.

EN ISO 13849-1:

This standard may be applied to safety-related parts of control systems and all types of machinery regardless of the type of technology and energy used (electrical, pneumatic, hydraulic, mechanical, etc).
Starting point for the assessment of the risk reduction

### Step 5
**Determination of the achieved performance level, selection of the subsystems**

The PL or SIL\(\text{(c)}\) shall be estimated for each selected SRP/CS and SRECS and/or combination of SRP/CS and SRECS that perform a safety function.

### Step 6
**Validation / verification**

Verification if the selected units or systems meet the requirements defined in the system design.

---

**EN ISO 13849-1**

- **Sensor**
  - fail-safe inductive ifm sensors
- **Logic**
  - AS-i Safety at Work
- **Actuator**
  - ifm evaluation units ifm safety controller

---

**Frequency and/or exposure to a hazard**

<table>
<thead>
<tr>
<th>Frequency and/or exposure to a hazard</th>
<th>Probability of hazardous event</th>
<th>Probability of avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 1 h</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>&gt; 1 h to ≤ 1 day</td>
<td>5</td>
<td>likely 4</td>
</tr>
<tr>
<td>&gt; 1 day to ≤ 2 wks</td>
<td>4</td>
<td>possible 3</td>
</tr>
<tr>
<td>&gt; 2 wks to ≤ 1 year</td>
<td>3</td>
<td>rarely 2</td>
</tr>
<tr>
<td>&gt; 1 year</td>
<td>2</td>
<td>negligible 1</td>
</tr>
</tbody>
</table>

**Class C = C + W + P**

<table>
<thead>
<tr>
<th>Class C</th>
<th>SIL2</th>
<th>SIL2</th>
<th>SIL2</th>
<th>SIL3</th>
<th>SIL3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11-13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14-15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**other measures**

- SIL1

---

**Operating time**

- time 2
- time 3

---

**SRECS or SRP/CS**

- Detection
- Logic
- Actuation
Overview ifm main catalogues:

- **Position sensors and object recognition**
  - Inductive sensors
  - Capacitive sensors
  - Magnetic sensors, cylinder sensors
  - Safety technology
  - Valve sensors
  - Photoelectric sensors
  - Object recognition
  - Encoders
  - Evaluation systems, power supplies
  - Connection technology

- **Fluid sensors and diagnostic systems**
  - Level sensors
  - Flow sensors
  - Pressure sensors
  - Temperature sensors
  - Diagnostic systems
  - Evaluation systems, power supplies
  - Connection technology

- **Bus systems**
  - Bus system AS-Interface
  - Power supplies
  - Connection technology

- **Identification systems**
  - Multicode reading systems
  - RF-identification systems
  - Power supplies
  - Connection technology

- **Control systems**
  - Control systems for mobile vehicles
  - Connection technology

ifm electronic – close to you!

Over 70 locations worldwide – at a glance at www.ifm.com

ifm electronic gmbh
Teichstraße 4
45127 Essen
Tel. +49 / 0201 / 2 42 20
Fax +49 / 0201 / 2 42 22 00
E-Mail: info@ifm.com